What is claimed is:

1 A Jacobian group element adder, which is an arithmetic unit for executing addition in a Jacobian group of an algebraic curve defined by a polynomial defined over a finite field that is

$$Y^3+\alpha_0X^4+\alpha_1XY^2+\alpha_2X^2Y+\alpha_3X^3+\alpha_4Y^2+\alpha_5XY+\alpha_6X^2+\alpha_7Y+\alpha_8X+\alpha_9$$

or

$$Y^2+\alpha_0X^5+\alpha_1X^2Y+\alpha_2X^4+\alpha_3XY+\alpha_4X^3+\alpha_5Y+\alpha_6X^2+\alpha_7X+\alpha_8$$

or

$$Y^2+\alpha_0X^7+\alpha_1X^3Y+\alpha_2X^6+\alpha_3X^2Y+\alpha_4X^5+\alpha_5XY+\alpha_6X^4+\alpha_7Y+\alpha_8X^3+\alpha_9X^2+\alpha_{10}X+\alpha_{11},$$

said Jacobian group element adder comprising:

means for inputting an algebraic curve parameter file having an order of a field of definition, a monomial order, and a coefficient list described as a parameter representing said algebraic curve;

means for inputting Groebner bases I_1 and I_2 of ideals of the coordinate ring of the algebraic curve designated by said algebraic curve parameter file, said Groebner bases representing elements of said Jacobian group;

ideal reduction means for, in the coordinate ring of the algebraic curve designated by said algebraic curve parameter file, performing arithmetic of producing a Groebner basis J of the ideal which is a product of the ideal that the Groebner basis I_1 generates, and the ideal

that the Groebner basis I_2 generates;

first ideal reduction means for, in the coordinate ring of the algebraic curve designated by said algebraic curve parameter file, performing arithmetic of producing a Groebner basis J^* of the ideal, which is smallest in the monomial order designated by said algebraic curve parameter file among the ideals equivalent to an inverse ideal of the ideal that the Groebner basis J generates; and

second ideal reduction means for, in the coordinate ring of the algebraic curve designated by said algebraic curve parameter file, performing arithmetic of producing a Groebner basis J^{**} of the ideal, which is smallest in the monomial order designated by said algebraic curve parameter file among the ideals equivalent to an inverse ideal of the ideal that the Groebner basis J^* generates, to output it.

2 The Jacobian group element adder according to claim 1, wherein said ideal composition means has:

linear-relation derivation means for, for a plurality of vectors v_1, v_2, ..., and v_n that were input, outputting a plurality of vectors $\{m_1=(m_{1,1}, m_{1,2}, \ldots, m_{1,n}), m_2=(m_{2,1}, m_{2,2}, \ldots, m_{2,n}), \ldots\}$ representing linear dependence relations

$\Sigma_i m_{j,i} v_i=0\,(j=1,2,\ldots)$ of all of them employing a discharging method;

an ideal type table that is composed of a record number field, an ideal type number field, an order field, and an ideal type field;

a monomial list table that is composed of the record number field, the order field, and a monomial list field;

a table for a Groebner basis construction that is composed of the record number field, the order field, a component number list field, a first vector type field, a second vector type field, and a third vector type field;

ideal type classification means for acquiring said algebraic curve parameter file to make a reference to said ideal type table for each of Groebner bases I_1 and I_2 that were input, to retrieve a record in which the ideal type described in the ideal type field accords with the type of an input ideal $I_i\,(i=1,2)$, and to acquire a value N_i of the ideal type number field and a value d_i of the order field of the retrieved record;

monomial vector generation means for calculating a sum $d_3=d_1+d_2$ of said values d_1 and d_2 of said order field to make a reference to said monomial list table for retrieving a record R of which a value of the order field is said d_3, to acquire a list M_1, M_2, … of the monomial described in said monomial list field of said record R,

when I_1 and I_2 are different, to calculate a remainder equation r_1 of dividing each said monomial M_i by I_1, to generate a vector $w^{(i)}{}_1$ that is composed of coefficients of the remainder equation r_i according to the monomial order described in said algebraic curve parameter file, furthermore to calculate a remainder equation s_i of dividing M_i by I_2, to generate a vector $w^{(i)}{}_2$ that is composed of coefficients of the remainder equation s_i according to the monomial order described in an algebraic curve parameter file A, to connect the above-mentioned two vectors $w^{(i)}{}_1$ and $w^{(i)}{}_2$ for generating a vector v_i, also, when I_1 and I_2 are equal, to calculate a remainder equation r_i of dividing each said monomial M_i by I_1, to generate a vector $w^{(i)}{}_1$ that is composed of coefficients of the remainder equation r_i according to the monomial order described in said algebraic curve parameter file, furthermore to construct a defining polynomial F employing the coefficient list and the monomial order described in said algebraic curve parameter file, when a differential of a polynomial M with regard to by its X is expressed by $D_X(M)$, and a differential of the polynomial M with regard to by its Y is expressed by $D_Y(M)$, to calculate a remainder equation s_i of dividing a polynomial $D_X(M_i)D_Y(F)-D_Y(M_i)D_X(F)$ by I_1, to generate a vector $w^{(i)}{}_2$ that is composed of coefficients of the remainder equation s_i

according to the monomial order described in said algebraic curve parameter file, and to connect the above-mentioned two vectors $w^{(i)}_1$ and $w^{(i)}_2$ for generating a vector v_i; and

basis construction means for inputting said plurality of said vectors v_1, v_2, … into said linear-relation derivation means, to acquire a plurality of vectors m_1, m_2, … as an output, to make an reference to said table for a Groebner basis construction for retrieving a record R_2, of which a value of the order field is said value d_3, and in which a vector of which the components that correspond to all component numbers described in the component number list field are all zero does not lie in said plurality of said vectors m_1, m_2, …, to select a vector m that accords with a first vector type of said record R_2 from among said plurality of said vectors m_1, m_2, …, to generate a polynomial f_1 of which the coefficient is a value of a component of the vector m according to the monomial order described in said algebraic curve parameter file, hereinafter, similarly, to generate a polynomial f_2 employing a vector that accords with a second vector type, and also a polynomial f_3 employing a vector that accords with a third vector type, to obtain a set $J=\{f_1, f_2, f_3\}$ of the polynomial, and to output it as said Groebner basis J.

3 The Jacobian group element adder according to one of claim 1 and claim 2, wherein each of said first and said second ideal reduction means has:

linear-relation derivation means for, for a plurality of vectors v_1, v_2, …, and v_n that were input, outputting a plurality of vectors $\{m_1=(m_{1,1},m_{1,2},\ldots,m_{1,n}),m_2=(m_{2,1},m_{2,2},\ldots,m_{2,n}),\ldots\}$ representing linear dependence relations $\Sigma_i m_{j,i}\, v_i=0(j=1,2,\ldots)$ of all of them employing a discharging method ;

an ideal type table that is composed of the record number field, the ideal type number field, a reduction order field, and the ideal type field;

a monomial list table that is composed of the record number field, the order field, and the monomial list field;

a table for a Groebner basis construction that is composed of the record number field, the order field, the component number list field, the first vector type field, the second vector type field, and the third vector type field;

ideal type classification means for acquiring said algebraic curve parameter file to make a reference to said ideal type table, to retrieve a record in which the ideal type described in the ideal type field accords with the

type of an input ideal J, to acquires a value N of the ideal type number field and a value d of the reduction order field of the retrieved record;

polynomial vector generation means for, when said d is zero, outputting the input ideal J as said Groebner basis J*, when said d is not zero, to make a reference to said monomial list table for retrieving a record R of which a value of the order field is said d, to acquire a list M_1, M_2, … of the monomial described in the monomial list field of said record R, to construct a defining polynomial F employing the coefficient list and the monomial order described in said algebraic curve parameter file, to acquire a first polynomial f, a second polynomial g, and a third polynomial h of the input ideal J, to calculate a remainder equation r_i of a product $M_i \cdot g$ of each said monomial M_i and the polynomial g by the polynomials f and F, to generate a vector $w^{(i)}{}_1$ that is composed of coefficients of the remainder equation r_i according to the monomial order described in said algebraic curve parameter file, furthermore to calculate a remainder equation s_i of a product $M_i \cdot h$ of each said monomial M_i and the polynomial h by the polynomials f and F, to generate a vector $w^{(i)}{}_2$ that is composed of coefficients of the remainder equation s_i according to the monomial order described in said algebraic curve parameter file, and to connect the above-

mentioned two vectors $w^{(i)}{}_1$ and $w^{(i)}{}_2$ for generating a vector v_i;

and basis construction means for inputting said plurality of said vectors v_1, v_2,… into said linear-relation derivation means, to obtain a plurality of vectors m_1, m_2, … as an output, to make a reference to said table for a Groebner basis construction for retrieving a record R_2 of which a value of the order field is said value d, and in which a vector of which the components that correspond to all component numbers described in the component number list field are all zero does not lie in said plurality of said vectors m_1, m_2, …, to select a vector m that accords with a first vector type of said record R_2 from among said plurality of said vectors m_1, m_2, …, to generate a polynomial f_1 of which a coefficient is a value of the component of the vector m according to the monomial order described in said algebraic curve parameter file, hereinafter, similarly, to generate a polynomial f_2 employing the vector that accords with a second vector type, and also a polynomial f_3 employing the vector that accords with a third vector type, to obtain a set $\{f_1, f_2, f_3\}$ of the polynomial, and to output it as said Groebner basis J* or J**.

4 A record medium having a program recorded for causing

an information processing unit configuring an arithmetic unit for executing addition in a Jacobian group of an algebraic curve defined by a polynomial defined over a finite field that is

$$Y^3+\alpha_0X^4+\alpha_1XY^2+\alpha_2X^2Y+\alpha_3X^3+\alpha_4Y^2+\alpha_5XY+\alpha_6X^2+\alpha_7Y+\alpha_8X+\alpha_9$$

or

$$Y^2+\alpha_0X^5+\alpha_1X^2Y+\alpha_2X^4+\alpha_3XY+\alpha_4X^3+\alpha_5Y+\alpha_6X^2+\alpha_7X+\alpha_8$$

or

$Y^2+\alpha_0X^7+\alpha_1X^3Y+\alpha_2X^6+\alpha_3X^2Y+\alpha_4X^5+\alpha_5XY+\alpha_6X^4+\alpha_7Y+\alpha_8X^3+\alpha_9X^2+\alpha_{10}X+\alpha_{11}$ to perform:

a process of inputting an algebraic curve parameter file having an order of a field of definition, a monomial order, and a coefficient list described as a parameter representing said algebraic curve;

a process of inputting Groebner bases I_1 and I_2 of ideals of the coordinate ring of the algebraic curve designated by said algebraic curve parameter file, said Groebner bases representing an element of said Jacobian group;

an ideal composition process of, in the coordinate ring of the algebraic curve designated by said algebraic curve parameter file, performing arithmetic of producing a Groebner basis J of an ideal which is a product of the ideal that the Groebner basis I_1 generates, and an ideal that the Groebner basis I_2 generates;

a first ideal reduction process of, in the coordinate ring of the algebraic curve designated by said algebraic curve parameter file, performing arithmetic of producing a Groebner basis J* of the ideal, which is smallest in the monomial order designated by said algebraic curve parameter file among the ideals equivalent to an inverse ideal of the ideal that the Groebner basis J generates; and

a second ideal reduction process of, in the coordinate ring of the algebraic curve designated by said algebraic curve parameter file, performing arithmetic of producing a Groebner basis J** of the ideal, which is smallest in the monomial order designated by said algebraic curve parameter file among the ideals equivalent to an inverse ideal of the ideal that the Groebner basis J* generates, to output it, said record medium being readable by said information processing unit.

5 The record medium according to claim 4, said record medium having a program recorded for causing said information processing unit to further perform in said ideal composition process:

a linear-relation derivation process of, for a plurality of vectors v_1, v_2, …, and v_n that were input, outputting a plurality of vectors

$\{m_1=(m_{1,1},m_{1,2},\ldots,m_{1,n}),m_2=(m_{2,1},m_{2,2},\ldots,m_{2,n}),\ldots\}$ representing linear dependence relations $\Sigma_i m_{j,i}\ v_i=0(j=1,2,\ldots)$ of all of them employing a discharging method;

an ideal type classification process of acquiring said algebraic curve parameter file to make a reference to an ideal type table, which is composed of a record number field, an ideal type number field, an order field, and an ideal type field, for each of Groebner bases I_1 and I_2 that were input, to retrieve a record in which the ideal type described in the ideal type field accords with the type of an input ideal $I_i(i=1,2)$, and to acquire a value N_i of the ideal type number field and a value d_i of the order field of the retrieved record;

a monomial vector generation process of calculating a sum $d_3=d_1+d_2$ of said values d_1 and d_2 of said order field to make a reference to a monomial list table, which is composed of the record number field, the order field, and a monomial list field, for retrieving a record R of which a value of the order field is said d_3, to acquire a list M_1, M_2, … of the monomial described in said monomial list field of said record R, when I_1 and I_2 are different, to calculate a remainder equation r_i of dividing each said monomial M_i by I_1, to generate a vector $w^{(i)}{}_1$ that is composed of coefficients of the remainder equation r_i

according to the monomial order described in said algebraic curve parameter file, furthermore to calculate a remainder equation s_i of dividing M_i by I_2, to generate a vector $w^{(i)}{}_2$ that is composed of coefficients of the remainder equation s_i according to the monomial order described in an algebraic curve parameter file A, to connect the above-mentioned two vectors $w^{(i)}{}_1$ and $w^{(i)}{}_2$ for generating a vector v_i, also, when I_1 and I_2 are equal, to calculate a remainder equation r_i of dividing each said monomial M_i by I_1, to generate a vector $w^{(i)}{}_1$ that is composed of coefficients of the remainder equation r_i according to the monomial order described in said algebraic curve parameter file, furthermore to construct a defining polynomial F employing the coefficient list and the monomial order described in said algebraic curve parameter file, when a differential of a polynomial M with regard to by its X is expressed by $D_X(M)$, and a differential of the polynomial M with regard to by its Y is expressed by $D_Y(M)$, to calculate a remainder equation s_i of dividing a polynomial $D_X(M_i)D_Y(F)-D_Y(M_i)D_X(F)$ by I_1, to generate a vector $w^{(i)}{}_2$ that is composed of coefficients of the remainder equation s_i according to the monomial order described in said algebraic curve parameter file, and to connect the above-mentioned two vectors $w^{(i)}{}_1$ and $w^{(i)}{}_2$ for generating a vector v_i; and

a basis construction process of obtaining a plurality of vectors m_1, m_2, … output in said linear-relation derivation process, to make an reference to a table for a Groebner basis construction, which is composed of the record number field, the order field, a component number list field, a first vector type field, a second vector type field, and a third vector type field, for retrieving a record R_2, of which a value of the order field is said value d_3, and in which a vector of which the components that correspond to all component numbers described in the component number list field are all zero does not lie in said plurality of said vectors m_1, m_2, …, to select a vector m that accords with a first vector type of said record R_2 from among said plurality of said vectors m_1, m_2, …, to generate a polynomial f_1 of which the coefficient is a value of a component of the vector m according to the monomial order described in said algebraic curve parameter file, hereinafter, similarly, to generate a polynomial f_2 employing a vector that accords with a second vector type, and also a polynomial f_3 employing a vector that accords with a third vector type, to obtain a set $J=\{f_1,f_2,f_3\}$ of the polynomial, and to output it as said Groebner basis J.

6 The record medium according to one of claim 4 and claim 5, said record medium having a program recorded for

causing said information processing to further perform in each of said first and second ideal reduction processes:

a linear-relation derivation process of, for a plurality of vectors v_1, v_2, …, and v_n that were input, outputting a plurality of vectors $\{m_1=(m_{1,1},m_{1,2},\ldots,m_{1,n}),m_2=(m_{2,1},m_{2,2},\ldots,m_{2,n}),\ldots\}$ representing linear dependence relations $\Sigma_i m_{j,i}\ v_i=0\,(j=1,2,\ldots)$ of all of them employing a discharging method ;

an ideal type classification process of acquiring said algebraic curve parameter file to make a reference to a ideal type table, which is composed of the record number field, the ideal type number field, a reduction order field, and the ideal type field, to retrieve a record in which the ideal type described in the ideal type field accords with the type of an input ideal J, and to acquire a value N of the ideal type number field and a value d of the reduction order field of the retrieved record;

a polynomial vector generation process of, when said d is zero, outputting the input ideal J as said Groebner basis J*, when said d is not zero, to make a reference to a monomial list table, which is composed of the record number field, the order field, and the monomial list field, for retrieving a record R of which a value of the order field is said d, to acquire a list M_1, M_2, … of the

monomial described in the monomial list field of said record R, to construct a defining polynomial F employing the coefficient list and the monomial order described in said algebraic curve parameter file, to acquire a first polynomial f, a second polynomial g, and a third polynomial h of the input ideal J, to calculate a remainder equation r_i of a product $M_i \cdot g$ of each said monomial M_i and said polynomial g by the polynomials f and F, to generate a vector $w^{(i)}{}_1$ that is composed of coefficients of the remainder equation r_i according to the monomial order described in said algebraic curve parameter file, furthermore to calculate a remainder equation s_i of a product $M_i \cdot h$ of each said monomial M_i and the polynomial h by the polynomials f and F, to generate a vector $w^{(i)}{}_2$ that is composed of coefficients of the remainder equation s_i according to the monomial order described in said algebraic curve parameter file, and to connect the above-mentioned two vectors $w^{(i)}{}_1$ and $w^{(i)}{}_2$ for generating a vector v_i; and

a basis construction process of obtaining a plurality of vectors m_1, m_2, … output in said linear-relation derivation process to make a reference to a table for a Groebner basis construction, which is composed of the record number field, the order field, the component number list field, the first vector type field, the second vector

type field, and the third vector type field, for retrieving a record R_2 of which a value of the order field is said value d, and in which a vector of which the components that correspond to all component numbers described in the component number list field are all zero does not lie in said plurality of said vectors m_1, m_2, …, to select a vector m that accords with a first vector type of said record R_2 from among said plurality of said vectors m_1, m_2, …, to generate a polynomial f_1 of which a coefficient is a value of the component of the vector m according to the monomial order described in said algebraic curve parameter file, hereinafter, similarly, to generate a polynomial f_2 employing the vector that accords with a second vector type, and also a polynomial f_3 employing the vector that accords with a third vector type, to obtain a set $\{f_1,f_2,f_3\}$ of the polynomial, and to output it as said Groebner basis J^* or J^{**}.